



Practitioner's Docket No. 915-008.11

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Haverinen Group No.:
Application No.: 10/601,337
Filed: June 20, 2003 Examiner:
For: Method, System and Devices for Transferring Accounting Information

Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country: PCT
Application PCT/IB02/02289
Number:
Filing Date: 20 June 2002

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 C.F.R. § 1.4(f) (emphasis added).


SIGNATURE OF PRACTITIONER

Reg. No. 27,550

Alfred A. Fressola

(type or print name of practitioner)

Tel. No. (203) 261-1234

Ware, Fressola, Van Der Sluys & Adolphson LLP

P.O. Address Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468

Customer No.: 004955

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent, if the foreign application is referred to in the oath or declaration, as required by § 1.63.

CERTIFICATE OF MAILING (37 C.F.R. § 1.8a)

I hereby certify that this correspondence is, on the date shown below is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.


Signature

Shannon Watt

(type or print name of person certifying)

Date: 10/31/03

(Transmittal of Certified Copy [5-4])

PCT REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only	
PCT / IB 0 2 / 0 2 2 8 9	
International Application No.	
20 JUNE 2002	20.06.02
International Filing Date	
INTERNATIONAL BUREAU OF WIPO	
Name of receiving Office and "PCT International Application"	
Applicant's or agent's file reference (if desired) (12 characters maximum)	2024128

Box No. I TITLE OF INVENTION	
METHOD, SYSTEM AND DEVICES FOR TRANSFERRING ACCOUNTING INFORMATION	
Box No. II APPLICANT <input type="checkbox"/> This person is also inventor.	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	Telephone No.
NOKIA CORPORATION Keilalahdentie 4 FI-02150 ESPOO FINLAND	Facsimile No.
	Teleprinter No.
	Applicant's registration No. with the Office
State (that is, country) of nationality: Finland	State (that is, country) of residence: Finland
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input checked="" type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	This person is:
HAVERINEN, Henry Arkkitehdinkatu 15 A 3 FI-33720 TAMPERE FINLAND	<input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.)
	Applicant's registration No. with the Office
State (that is, country) of nationality: Finland	State (that is, country) of residence: Finland
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<input checked="" type="checkbox"/> Further applicants and/or (further) inventors are indicated on a continuation sheet	
Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE	
The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	<input checked="" type="checkbox"/> agent <input type="checkbox"/> common representative
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	Telephone No.
AWAPATENT AB Box 5117 SE-200 71 MALMÖ SWEDEN	+46 40 98 51 00
	Facsimile No.
	+46 40 26 05 16
	Teleprinter No.
	Agent's registration No. with the Office
<input type="checkbox"/> Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent	

Sheet No. 2

Continuation of Box No. III		FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
If none of the following sub-boxes is used, this sheet should not be included in the request.			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) ASOKAN, Nadarajah Ankkurinvarsi 6 K FI-02320 ESPOO FINLAND^A		This person is: <input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality: Canada		State (that is, country) of residence: Finland	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States		<input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) LAITINEN, Pekka Hiihtomäentie 44 A 2 FI-00800 HELSINKI FINLAND^A		This person is: <input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality: Finland		State (that is, country) of residence: Finland	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States		<input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) (Empty)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States		<input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) (Empty)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States		<input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<input type="checkbox"/> Further applicants and/or (further) inventors are indicated on another continuation sheet.			

Form PCT/RO/101 (continuation sheet) (March 2001; reprint January 2002)

See Notes to the request form

Sheet No. 3

Box No. V DESIGNATION OF STATES Mark the applicable check-boxes below; at least one must be marked.

The following designations are hereby made under Rule 4.9(a):

Regional Patent

- ☒ AP ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZM Zambia, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT (if other kind of protection or treatment desired, specify on dotted line)
- ☒ EA Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ EP European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ OA OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, EQ Equatorial Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> AE United Arab Emirates | <input checked="" type="checkbox"/> GM Gambia | <input checked="" type="checkbox"/> NZ New Zealand |
| <input checked="" type="checkbox"/> AG Antigua and Barbuda | <input checked="" type="checkbox"/> HR Croatia | <input checked="" type="checkbox"/> OM Oman |
| <input checked="" type="checkbox"/> AL Albania | <input checked="" type="checkbox"/> HU Hungary | <input checked="" type="checkbox"/> PH Philippines |
| <input checked="" type="checkbox"/> AM Armenia | <input checked="" type="checkbox"/> ID Indonesia | <input checked="" type="checkbox"/> PL Poland |
| <input checked="" type="checkbox"/> AT Austria +Utility Model | <input checked="" type="checkbox"/> IL Israel | <input checked="" type="checkbox"/> PT Portugal |
| <input checked="" type="checkbox"/> AU Australia | <input checked="" type="checkbox"/> IN India | <input checked="" type="checkbox"/> RO Romania |
| <input checked="" type="checkbox"/> AZ Azerbaijan | <input checked="" type="checkbox"/> IS Iceland | <input checked="" type="checkbox"/> RU Russian Federation |
| <input checked="" type="checkbox"/> BA Bosnia and Herzegovina | <input checked="" type="checkbox"/> JP Japan | |
| <input checked="" type="checkbox"/> BB Barbados | <input checked="" type="checkbox"/> KE Kenya | <input checked="" type="checkbox"/> SD Sudan |
| <input checked="" type="checkbox"/> BG Bulgaria | <input checked="" type="checkbox"/> KG Kyrgyzstan | <input checked="" type="checkbox"/> SE Sweden |
| <input checked="" type="checkbox"/> BR Brazil | <input checked="" type="checkbox"/> KP Democratic People's Republic of Korea | <input checked="" type="checkbox"/> SG Singapore |
| <input checked="" type="checkbox"/> BY Belarus | <input checked="" type="checkbox"/> KR Republic of Korea | <input checked="" type="checkbox"/> SI Slovenia |
| <input checked="" type="checkbox"/> BZ Belize | <input checked="" type="checkbox"/> KZ Kazakhstan | <input checked="" type="checkbox"/> SK Slovakia +Utility Model |
| <input checked="" type="checkbox"/> CA Canada | <input checked="" type="checkbox"/> LC Saint Lucia | <input checked="" type="checkbox"/> SL Sierra Leone |
| <input checked="" type="checkbox"/> CH & LI Switzerland and Liechtenstein | <input checked="" type="checkbox"/> LK Sri Lanka | <input checked="" type="checkbox"/> TJ Tajikistan |
| <input checked="" type="checkbox"/> CN China | <input checked="" type="checkbox"/> LR Liberia | <input checked="" type="checkbox"/> TM Turkmenistan |
| <input checked="" type="checkbox"/> CO Colombia | <input checked="" type="checkbox"/> LS Lesotho | <input checked="" type="checkbox"/> TN Tunisia |
| <input checked="" type="checkbox"/> CR Costa Rica | <input checked="" type="checkbox"/> LT Lithuania | <input checked="" type="checkbox"/> TR Turkey |
| <input checked="" type="checkbox"/> CU Cuba | <input checked="" type="checkbox"/> LU Luxembourg | <input checked="" type="checkbox"/> TT Trinidad and Tobago |
| <input checked="" type="checkbox"/> CZ Czech Republic +Utility Model | <input checked="" type="checkbox"/> LV Latvia | <input checked="" type="checkbox"/> TZ United Republic of Tanzania |
| <input checked="" type="checkbox"/> DE Germany +Utility Model | <input checked="" type="checkbox"/> MA Morocco | <input checked="" type="checkbox"/> UA Ukraine |
| <input checked="" type="checkbox"/> DK Denmark +Utility Model | <input checked="" type="checkbox"/> MD Republic of Moldova | <input checked="" type="checkbox"/> UG Uganda |
| <input checked="" type="checkbox"/> DM Dominica | <input checked="" type="checkbox"/> MG Madagascar | <input checked="" type="checkbox"/> US United States of America |
| <input checked="" type="checkbox"/> DZ Algeria | <input checked="" type="checkbox"/> MK The former Yugoslav Republic of Macedonia | <input checked="" type="checkbox"/> UZ Uzbekistan |
| <input checked="" type="checkbox"/> EC Ecuador | <input checked="" type="checkbox"/> MN Mongolia | <input checked="" type="checkbox"/> VN Viet Nam |
| <input checked="" type="checkbox"/> EE Estonia +Utility Model | <input checked="" type="checkbox"/> MW Malawi | <input checked="" type="checkbox"/> YU Yugoslavia |
| <input checked="" type="checkbox"/> ES Spain | <input checked="" type="checkbox"/> MX Mexico | <input checked="" type="checkbox"/> ZA South Africa |
| <input checked="" type="checkbox"/> FI Finland +Utility Model | <input checked="" type="checkbox"/> MZ Mozambique | <input checked="" type="checkbox"/> ZM Zambia |
| <input checked="" type="checkbox"/> GB United Kingdom | <input checked="" type="checkbox"/> NO Norway | <input checked="" type="checkbox"/> ZW Zimbabwe |
| <input checked="" type="checkbox"/> GD Grenada | | |
| <input checked="" type="checkbox"/> GE Georgia | | |
| <input checked="" type="checkbox"/> GH Ghana | | |

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)

Form PCT/RO/101 (second sheet) (January 2002)

See Notes to the request form

Sheet No. 4

Box No. VI PRIORITY CLAIM				
The priority of the following earlier application(s) is hereby claimed:				
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application:* regional Office	international application: receiving Office
item (1)				
item (2)				
item (3)				
item (4)				
item (5)				

☐ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

☐ all items
 ☐ item (1)
 ☐ item (2)
 ☐ item (3)
 ☐ item (4)
 ☐ item (5)
 ☐ other, see Supplemental Box

* Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):

Box No. VII INTERNATIONAL SEARCHING AUTHORITY		
Choice of International Searching Authority (ISA) (if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):		
ISA / <u>SE</u>		
Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority):		
Date (day/month/year)	Number	Country (or regional Office)

Box No. VIII DECLARATIONS		
The following declarations are contained in Boxes Nos. VIII (i) to (v) (mark the applicable check-boxes below and indicate in the right column the number of each type of declaration):		Number of declarations
<input type="checkbox"/> Box No. VIII (i)	Declaration as to the identity of the inventor	:
<input type="checkbox"/> Box No. VIII (ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	:
<input type="checkbox"/> Box No. VIII (iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	:
<input type="checkbox"/> Box No. VIII (iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America)	:
<input type="checkbox"/> Box No. VIII (v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	:

Form PCT/RO/101 (third sheet) (March 2001; reprint January 2002)

See Notes to the request form

Sheet No. 5

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application contains:

- (a) the following number of sheets in paper form:
- request (including declaration sheets) : 5
- description (excluding sequence listing part) : 23
- claims : 8
- abstract : 1
- drawings : 7
- Sub-total number of sheets : 44

sequence listing part of description (*actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (b) below*) :

Total number of sheets : 44

- (b) sequence listing part of description filed in computer readable form

- (i) ☐ only (under Section 801(a)(i))
- (ii) ☐ in addition to being filed in paper form (under Section 801(a)(ii))

Type and number of carriers (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained (*additional copies to be indicated under item 9(ii), in right column*):

This international application is accompanied by the following item(s) (mark the applicable check-boxes below and indicate in right column the number of each item):

1. ☐ fee calculation sheet :
 2. ☐ original separate power of attorney :
 3. ☐ original general power of attorney :
 4. ☒ copy of general power of attorney; reference number, if any: GPA 02/0021 : 1
 5. ☐ statement explaining lack of signature :
 6. ☐ priority document(s) identified in Box No. VI as item(s): :
 7. ☐ translation of international application into (language): :
 8. ☐ separate indications concerning deposited microorganism or other biological material :
 9. ☐ sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other)) :
 (i) ☐ copy submitted for the purposes of international search under Rule 13ter only (and not as part of the international application) :
 (ii) ☐ (only where check-box (b)(i) or (b)(ii) is marked in left column) additional copies including, where applicable, the copy for the purposes of international search under Rule 13ter :
 (iii) ☐ together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column :
 10. ☐ other (specify): :

Figure of the drawings which should accompany the abstract : 6


Language of filing of the international application: **English**

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Helsingborg, 20 June 2002

AWAPATENT AB


Jonas Delander

Authorized Representative

For receiving Office use only

1. Date of actual receipt of the purported international application: 20 JUNE 2002	2. Drawings: <input type="checkbox"/> received: <input type="checkbox"/> not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA SE	6. <input checked="" type="checkbox"/> Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

Form PCT/RO/101 (last sheet) (March 2001; reprint January 2002)

See Notes to the request form

METHOD, SYSTEM AND DEVICES FOR TRANSFERRING ACCOUNTING
INFORMATION

Technical Field of the Invention

The invention relates to a method in a system and a system for transfer of accounting information. Further,
5 the invention relates to a method in a terminal, a terminal, an Extensible Authentication Protocol (EAP) service authorization server, a method in an EAP service authorization server, a computer program, and an EAP sub type.

10

Background of the Invention

In Local Area Networks an operator of a service may be interested in providing themselves with a variety of accounting information related to the users utilizing the
15 network for accessing different services. Examples of such accounting information may be a value indicating for how long a user has utilized a specific service, a value indicating the amount of data received from and/or sent to a specific service, information regarding when the
20 user utilized the service, and/or the number of and/or the type of transactions performed.

Today there are systems in which the access points of the network collects accounting information for each user/terminal connecting to the network via the access
25 point. The access points then sends the information to an Authentication Authorization Accounting (AAA) server by means of an AAA protocol like RADIUS or DIAMETER.

However, there may be lack of trust between a service provider, who manages a service utilized by a
30 user, and an operator of a home network, who bill the user for utilized services. Thus, accounting information from the service provider has to be verified and

authorized before it is sent to the AAA-server of the operator of the home network.

Summary of the Invention

5 It is an object of the present invention to provide improved delivery of accounting information.

This object is accomplished by means of a method in a system for transferring accounting information according to claim 1, a system for transferring
10 accounting information according to claim 11, a method in a terminal according to claim 19, a terminal according to claim 22, a method in an Extensible Authentication Protocol (EAP) service authorization server according to claim 25, an EAP service authorization server according to
15 to claim 31, a computer program according to claim 35, a computer program according to claim 36, an Extensible Authentication Protocol response (EAP-response) packet according to claim 37. Preferred embodiments of the invention are disclosed in the dependent claims.

20 More particularly, according to one aspect, a method in a system for transferring accounting information comprises:

metering data related to a service used by at least one terminal,

25 providing the metered data as accounting information to at least one Extensible Authentication Protocol (EAP) service authorization server,

sending, by means of an Extensible Authentication Protocol request (EAP-request), a service authorization
30 request from said at least one EAP service authorization server to said at least one terminal,

digitally signing accounting information, in said at least one terminal,

including, at said at least one terminal, the
35 digitally signed accounting information in an Extensible Authentication Protocol response (EAP-response), and

sending the digitally signed accounting information to an AAA-server.

According to another aspect, a system for transferring accounting information comprises:

5 a metering server for metering data related to a service,

an Extensible Authentication Protocol (EAP) service authorization server including a generator for generating Extensible Authentication Protocol request (EAP-request) service authorizations, and a network connection means,

10 a terminal including a signer arranged to digitally sign verified accounting information, an Extensible Authentication Protocol response (EAP-response) generator arranged to insert verified and digitally signed accounting information in EAP-responses, and a network connection means, and

15 an Authentication Authorization Accounting server arranged to manage accounting information relating to at least one terminal.

20 According to yet another aspect, a method in a terminal comprises:

collecting data corresponding to accounting information relevant for at least one service presently utilized in the terminal,

25 receiving an Extensible Authentication Protocol request (EAP-request) including accounting information relevant for said at least one service presently utilized in the terminal,

30 comparing said received accounting information with the collected data, and,

if the collected data corresponds with the accounting information said method further comprising:

digitally signing said received accounting information, and

35 sending the digitally signed accounting information in an Extensible Authentication Protocol response (EAP-response).

4

According to a further aspect, a terminal comprises:
a collector arranged to collect data corresponding
to accounting information relevant for at least one
service presently utilized in the WLAN terminal,

5 a comparing device arranged to compare the collected
data with received accounting information,

a signer arranged to digitally sign verified
accounting information,

10 an Extensible Authentication Protocol response (EAP-
response) generator arranged to insert digitally signed
accounting information in EAP-responses, and

a network connection means.

According to yet another aspect, a method in an
Extensible Authentication Protocol (EAP) service
15 authorization server, said method comprises:

receiving accounting information related to at least
one terminal,

inserting said accounting information in an
Extensible Authentication Protocol request (EAP-request),

20 and
sending said EAP-request to the at least one terminal.

According to yet another aspect, an Extensible
Authentication Protocol (EAP) service authorization
server comprises:

25 an accounting information receiver for receiving
accounting information relating to at least one terminal,

an Extensible Authentication Protocol request (EAP-
request) generator arranged to insert accounting
information of at least one terminal in an EAP-request,

30 and

a network connection means.

By making the terminal/user authorize the accounting
information by using EAP to initiate said authorization
and to transport signed accounting information from said
35 terminal/user it may be possible to provide authorization
of accounting information by the user or the terminal of
the user without requiring much extra effort from an

5

access network operator, a service operator, or the user in regard of modifying existing systems. In many cases it may be an advantage that EAP already exist, thus, no need to implement or develop additional protocols. Further the
5 EAP service authorization server establishes contact with the terminal during the establishment of a connection to the access network, thus, there is no need to use server discovery protocols, client IP address discoveries, or other similar procedures. Also, the EAP message including
10 the service authorization is able to traverse personal firewalls and Virtual Private Network (VPN) clients in the terminal.

By making it possible for the user/terminal to authorize the accounting information the correctness of
15 the accounting information may be guaranteed, and the uncertainty of account information sent directly from an operator of the access network, which operator may or may not be trustworthy, is eliminated. Thus, an operator of the access network, or any other service, is not able to
20 forge the accounting information and thereby the user may not later on repudiate the accounting information. Further, this may also make a user feel more comfortable in using services that costs money, because the user is to some extent in control of the debiting procedure and
25 not totally in the hands of the operators.

In the context of the invention service is a service that is possible to access by means of a terminal via a service provider. For example a service may include access to one or a plurality of network environments,
30 e.g. a local network, a private network, the Internet, a specific operator controlled network, or a virtual local area network, and it may include access different facilities, e.g. facilities for e-mail, facilities for Short Message Service (SMS), facilities for Multi Media
35 Service (MMS), facilities for e-commerce, printing facilities, etc.

According to one embodiment the metering server and the EAP service authorization server is comprised in the same device, e.g. an access point. This may increase the available bandwidth in a access network because

5 information exchange between the metering server and the EAP service authorization server no longer needs to utilize the network, e.g. the amount of protocol messages sent may decrease.

According to another embodiment the metering server
10 and the EAP service authorization server is comprised in different devices. This feature may facilitate introduction of an EAP service authorization server in a network system that already includes a metering server. For example in a Wireless LAN including access points
15 that supports Radius accounting or any other accounting protocol.

In one embodiment the EAP-request and the EAP-response is sent over a WLAN connection.

In another embodiment the EAP-response including the
20 signed account information from the terminal is sent to, or received by, the EAP service authorization server. This makes it possible for the operator of the access network to check that the user of the terminal or the terminal has not tampered with the accounting
25 information. Additionally, the operator of the access network may control the identity of the user of the terminal if necessary.

In yet another embodiment the signing and the verification of a signature is performed by means of a
30 public key crypto system.

A further scope of applicability of the present invention will become apparent from the detailed description given below. However, it should be understood that the detailed description and specific examples,
35 while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of

the invention will become apparent to those skilled in the art from this detailed description.

Brief Description of the Drawings

5 Other features and advantages of the present invention will become apparent from the following detailed description of a presently preferred embodiment, with reference to the accompanying drawings, in which

Fig. 1 shows a schematic overview of a system
10 according to one embodiment,

Fig. 2 shows a schematic view of one embodiment of a terminal,

Fig. 3 shows a flowchart of a process for handling accounting information in the terminal of Fig. 2,

15 Fig. 4 shows a schematic view of one embodiment of a EAP service authorization server,

Fig. 5 shows a flowchart of a process for handling accounting information and,

20 Fig. 6 shows a timing diagram over messages sent during a transmission of account information according to one embodiment,

Fig. 7 shows a timing diagram over messages sent during a transmission of accounting information according to another embodiment,

25 Fig. 8 shows a schematic view of the format of an embodiment of an EAP-Request/Service-Authorization packet and an EAP-Response/Service-Authorization packet,

Fig. 9 shows a schematic view of the format of another embodiment of an EAP-Request/Service-
30 Authorization packet and an EAP-Response/Service-Authorization packet, and

Fig. 10 shows a schematic view of a Flags field of a packet according to Fig. 9.

35 Detailed Description of an Embodiment

In Fig. 1 a schematic overview of a system according to one embodiment is shown. The system comprises an

Extensible Authentication Protocol (EAP) Service authorization server 10, an access point 12, an Authentication Authorization Accounting (AAA) server 14, and a terminal 16.

5 In one embodiment the communication between a access point 12, an EAP Service authorization server 10, and an AAA-server 14 is performed via a network 18.

The EAP Service authorization server 10 is arranged to provide the terminal 16 with accounting information
10 that the terminal may verify. The EAP Service authorization server 10 may, for example, be arranged as a separate server, included in the access point 12, included in the AAA-server 14, or included in any other device that is able to communicate with the terminal 16,
15 the AAA-server 14 and the access point 12.

The AAA-server 14 may be any type of AAA-server that is known to a person skilled in the art.

The access point 12 may be any type of access point that is known to a person skilled in the art. The
20 access point 12 includes means for metering account information related to one or a plurality of terminals connecting via it. Thus, one may say that it includes a metering server. The access point 12 is arranged to send and receive data by means of wireless communication, e.g.
25 Wireless Local Area Network communication, infrared communication, Bluetooth, or any radio based communication. In one embodiment the access point 12 is an access point that operates in accordance with the IEEE 802 standard and that utilizes an Extensible
30 Authentication Protocol (EAP) according to IEEE 802.1x.

The terminal may be any device having an user interface and means for performing communication. For example the terminal may be a telephone, a Personal Digital Assistant (PDA), a handheld computer, a laptop
35 computer, a desktop computer. The terminal may be arranged to communicate via a wireless communication channel, as shown in Fig. 1, or via a wire, not shown in

Fig. 1. The wireless communication may, for example, be Wireless Local Area Network communication, infrared communication, Bluetooth, or any radio based communication. The communication via a wire may, for example, be communication via a modem and a telephone network, a direct connection to a Local Area Network. In a system where there are terminals connected to the network via wires there may be arranged a separate metering server for collecting the accounting information.

In one embodiment the access point 12 is part of an access network that is managed by an access network operator and the AAA-server is part of an accounting management system managed by an AAA-server operator or an home operator. The access network operator and the home operator may be part of the same organization or different organizations.

The service authorization may relate to a network access, but, it may also relate to a printer service in which a user, for example, pay per printed page, a e-commerce service in which a user, for example pay for the ordered service or product, etc.

In Fig. 2 one embodiment of a terminal 16 is shown. The terminal 16 comprises a connection means 202 for wireless connection to and communicating via an access point, and a protocol stack 204 comprising an EAP 206. However, as mentioned above the connection means may be a modem or an ordinary network interfacing card for connecting to said network by means of a wire. Further, the terminal 16 comprises a collector 208 for collecting data corresponding to accounting information relevant for at least one service presently utilized in the terminal, a verifier 210 for verifying that the accounting information received from the corresponds to the collected data, a signer 212 for signing accounting information that has been approved by the comparing means, and an EAP-response generator 214 for inserting

signed accounting information into an EAP-response message.

In one embodiment the collector collects an input from an user stating whether the user accepts the accounting information or not. Then, in such embodiment, the verifier only has to check the collected input from the user in order to decide whether the verification is a success or not.

The signer 212 may comprise means for performing any type of digitally signing known to a person skilled in the art, e.g. it may be a public key cryptosystem, which normally is used for signing, or it may be a symmetric encryption system. In a public key crypto system there is one private and one public key. The public key may be distributed to all involved parties. The signer then encrypts a message by means of the private key. If said message then is possible to decrypt using the public key the signature is verified as being the signature of the person having the public key.

The means 202-214 described above may be entirely or partially implemented by means of software code.

The accounting information may be a value indicating for how long time the terminal has been connected to a service, a value indicating the amount of data sent and/or received using a specific service, information regarding when the user utilized the service, the number of and/or the type of transactions performed, and/or the number of service utilizations.

In Fig. 3 a process in one embodiment of the terminal is shown. The process starts when the terminal receives an EAP-request for service authorization including accounting information, step 300. Then the accounting information is extracted from the EAP-request, step 302. When the accounting information is available in the terminal a process of verifying starts, step 304.

The step of verifying may be performed in many ways. In one embodiment the terminal collects data

11

corresponding to the accounting information for a service presently in use during essentially the entire period when the service is used. Then, when the verifying step 304 is performed the terminal compares the collected data with the received accounting information and makes a decision based on the difference between the collected data and the received accounting information regarding whether the verification of the accounting information is successful or not.

10 In another embodiment the received accounting information the terminal does not perform the comparison, but presents the accounting information and the collected data for the user who decides whether to verify the accounting information or not. If the user verifies then the step of verifying 304 is a success, else it is a failure.

20 In yet another embodiment the terminal do not collect said data and, thus, no collected data is available. In such case the step of verifying 304 may present the received accounting information for the user and wait for him to verify the accounting information. If the user verifies then the step of verifying 304 is a success, else it is a failure.

25 In a further embodiment the terminal collects data and compares the data with the received accounting information. However, the terminal provides an interface for the user by means of which the user may select "ok" or "cancel" in order to accept the accounting information or prevent it from being sent. The signing of the accounting information may be performed before or after the user has notified the terminal of the selection.

35 In another embodiment the EAP-request for service authorization, received in step 300, do not include any accounting information. In such case the step 302 regarding extracting accounting information is not performed. After receipt of the EAP-request for service authorization, the terminal regard data collected by

itself as verified accounting information and, thus, the step of verification regarded as a success.

In step 306, independent of which of the above embodiments of the verifying step 304 that is used, the process checks whether the verifying step 304 resulted in a success or a failure. If the result is a failure then the process is ended, step 308. However, if the result is a success then the process proceeds by signing the accounting information, step 310.

The signing, step 310, may be performed by means of any method known by a person skilled in the art. For example, by means of public key encryption. Also other signing schemes may be used, e.g. a symmetric cryptography system may be used to encrypt the accounting information, however, in such case only the terminal and the home operator may share the key of representing the signature.

Then the signed accounting information is inserted in an EAP-response, step 314, and the EAP-response is sent via the network connection.

In Fig. 4 one embodiment of the EAP service authorization server is shown 10. The EAP service authorization server according to the figure comprises network connection means 402 for connecting to a network 403, and a protocol stack 404 including a EAP 406. If the EAP service authorization server 10 is not a device in which only the EAP service authorization server 10 is implemented the network connection means 402 and the protocol stack 404 may be shared by the other devices, e.g. if the EAP service authorization server 10 is included in a access point, in an AAA server, or in a AAA proxy server. In one embodiment the stack also includes an AAA protocol, e.g. RADIUS protocol or a DIAMETER protocol.

Further, the EAP service authorization server 10 includes an accounting information receiver 408, which is arranged to manage accounting information received from

13

one or a plurality of access points, and an EAP-request generator, which is arranged to utilize EAP 406 and generate EAP-requests for service authorizations.

According to one embodiment the EAP-request includes
5 accounting information of a specific terminal for sending to said specific terminal, this is implemented if the terminal or user is to make the decision regarding whether the accounting information from the EAP service authorization server is correct or not. According to
10 another embodiment the EAP-request for service authorization do not include any accounting information, this is implemented if the EAP service authorization server is to make the decision regarding whether the accounting information from the terminal is correct or
15 not.

The time between sending two consecutive EAP-requests including accounting information of a specific terminal may be based the time between reception of accounting information, a value of a specific property of
20 the accounting information, e.g. said EAP-request is to be sent when the time passed since the last request exceeds a specific value or when the amount of data sent and/or received since the last request exceeds a specific value, or a predetermined criteria set by one of the
25 operators. The EAP service authorization may be arranged to handle accounting information relating to one or a plurality of terminals.

Further, the EAP service authorization server 10 includes an extractor 412, a signature verifier 414, an
30 access terminator 416, and an accounting message generator 418.

The extractor 412 is arranged to extract signed accounting information from an EAP-response originating from an terminal.

35 The verifier 414 is arranged to verify the signature and the content of the EAP-response message. Verification of the content may be achieved by checking if the

14

received accounting information corresponds to information sent from the EAP service authorization server to the terminal or if the received information corresponds to information collected at the EAP service authorization server. Verification of the signature may be achieved by means of a public key stored in the EAP service authorization server 10. The public key may have been provided to the EAP service authorization server 10 from the terminal in the form of a certificate in an EAP-response, or from the AAA server in a Diameter/Radius EAP-Answer message during the access authorization process.

The access terminator 416 is arranged to terminate the access to a specific service if one or a plurality of predetermined criteria are not met.

The accounting message generator is arranged to generate an AAA-message including signed accounting information and initiate sending of the message to an AAA-server managing the service that the accounting information is related to.

In Fig. 5 a process of one embodiment of the EAP service authorization server 10 is shown. The process starts when the EAP service authorization server 10 receives accounting information related to a specific terminal, step 502. Then, an EAP-request is generated, the EAP-request includes said accounting information, step 504. Then the EAP-request is sent to said terminal, which the accounting information relates to, step 506. In one embodiment the generation and sending of the EAP-request including the accounting information is not performed until the accumulated value of a specific property in the accounting information has been reached, e.g. a time value, a value of sent and/or received data, or a value relating directly to money, i.e. the sending may be performed periodically or once in a certain period of time.

15

When the EAP-request is sent a timer is started, step 508. In step 510 the value of the timer is compared with a predetermined time limit, t_{limit} . If the value of the timer does not exceed t_{limit} then the process continues
5 by checking whether an EAP-response has been received from the terminal, step 514. If no EAP-response has been received the process returns to step 510 and compare the value of the timer with the value of t_{limit} . If the value of the timer exceed the value of t_{limit} , then no EAP-
10 response has been received within the time limit and the process continues to step 512 and ends the access to the service that the accounting information relates to. However, if an EAP-response is received, step 514, before the time limit runs out the EAP service authorization
15 server 10 verifies the signature in the EAP-response, step 516, by means of the signature of the terminal or the user of the terminal that is stored in a memory of the EAP service authorization server 10. The process may also verify that the received accounting information
20 corresponds to the accounting information sent to the terminal. If the signature is not valid, step 518, the process continues to step 512 and ends the access to the service that the accounting information relates to. However if the signature is valid the process continues
25 to step 520, where it prepares and sends the signed account information to an AAA-server.

According to another embodiment, the EAP-request generated in step 504 does not include the accounting information and ,thus, the accounting information
30 received in the EAP-response, step 514, is information collected by the terminal. Thus, the verification of content in step 516 is performed by comparing the received accounting information with corresponding accounting information collected at the EAP service
35 authorization server.

In Fig. 6 there is shown a timing diagram according to one embodiment in which the EAP service authorization

16

server is arranged as a separate device, in a AAA-proxy, or in another suitable device. According to this embodiment an access point collects accounting information for one or a plurality of users/terminals.

- 5 For each user/terminal the access point collects data at least during the time period the terminal is accessing a service, 602. When accounting information has been collected during a predetermined period of time or for a predetermined amount of sent and/or received data, the
- 10 access point sends a Diameter accounting request, 604, including the accounting information related to a specific terminal to an EAP service authorization server. The accounting request is not necessarily sent by means of the Diameter protocol, but may be sent by means of any
- 15 protocol that may be used to achieve a corresponding functionality, e.g. the RADIUS protocol. This also apply for other transmissions mentioned below as using the Diameter protocol.

- The EAP service authorization server then manages
- 20 the Diameter accounting request, message 604, see Figs 4 and 5, and the included accounting information and respond by sending a Diameter EAP-answer, message 606, to the access point. The Diameter EAP-answer includes an EAP-request/Service-Authorization that carries accounting
- 25 information. The EAP-request/Service-Authorization message carrying the accounting information is then packed by the EAP over LAN (EAPOL) protocol at the access point and is sent as any other EAP-request to said specific terminal, message 608. In the depicted
- 30 embodiment the terminal is a Wireless Lokal Area Network (WLAN) enabled terminal. However, as mentioned above, the terminal may be arranged for communication by means of other methods. The terminal then manages the received EAP-Request, checks the accounting information 609, also
- 35 see Figs 2 and 3, and sends an EAPOL including an EAP-Response/Service-Authorization that carries signed accounting information to the access point, message 610.

17

The sending of the EAPOL including the EAP-Response/Service-Authorization that carries signed accounting information is only performed if the verification of the accounting information was successful. The access point then pass the EAP-Response/Service-Authorization, carrying the signed accounting information, to the EAP service authorization server by means of a Diameter EAP-Request, message 612. Then the EAP service authorization server generates an EAP-success message and sends it in an Diameter EAP-answer to the access point, message 614. The access point then pass the EAP-success message on to the terminal by means of an EAPOL, message 616. When the signed accounting information is received at the EAP service authorization server in message 612, the EAP service authorization server starts to verify the signature of the accounting information 617, also see Figs 4 and 5. If the verification of the signature is successful, i.e. the signature is valid, then the EAP service authorization server sends a Diameter Accounting-Request including the signed accounting information to an AAA server that is to manage the accounting information.

In Fig. 7 there is shown a timing diagram according to another embodiment in which the EAP service authorization server is included in the access point. In this embodiment the account information collected or measured 702 by means of the access point is accessible for the EAP service authorization server or is passed to the EAP service authorization server by means of internal communication within the access point. Then the Access point/EAP service authorization server generate and sends an EAPOL message including an EAP-Request/Service-Authorization carrying the accounting information, message 704, to the terminal. In the depicted embodiment the terminal is a WLAN enabled terminal. However, as mentioned above, the terminal may be arranged for communication by means of other methods. In the terminal

18

the accounting information is verified 706. If the verification is successful then the accounting information is signed and the terminal sends an EAPOL message 708 including an EAP-Response/Service-
5 Authorization, which is carrying the signed accounting information, to the access point. In response to this message the access point responds by sending an EAPOL message including an EAP-Success message 710. Then the access point/EAP service authorization server generates
10 and sends a Diameter Accounting-Request 714 to the AAA server.

In Fig. 8 an embodiment of an EAP sub type in the form of an EAP-packet format specialized for EAP-Request/Service-Authorization and EAP-Response/Service-
15 Authorization is showed. The EAP-Request/Service-Authorization and EAP-Response/Service-Authorization packet both comprises a Code field 802, an Identifier field 804, a Length field 806, a Type field 808, a Data type field 810, and a Data field 812.

20 As in the EAP specification the length of the Code field 802 is 8 bits, i.e. one octet, and identifies the type of EAP-packet that are to be sent. EAP-codes are assigned as follows:

- | | | |
|----|---|----------|
| 25 | 1 | Request |
| | 2 | Response |

Other codes used in the Code field 802 of EAP-packets are 3 for Success and 4 for Failure. However for these codes the format of the EAP-packet do not necessary
30 correspond to the format of the EAP-Request/Service-Authorization and EAP-Response/Service-Authorization as shown in Fig. 8. A specific format for EAP-Success and EAP-Failure packets may be found in the specification of EAP contained in IETF RFC 2284.

35 The Identifier field 804 is also one octet and includes an identification code for matching responses

with requests. Generation of such identification codes is known by the skilled person.

The Length field 806 is two octets and indicates the length of the EAP packet including the Code field 802, the Identifier field 804, the Length field 806, the Type field 808, the Data type field 810, and the Data field 812.

The Type field 808 is one octet and specifies the type of the EAP packet. For the EAP-Request/Service-Authorization and EAP-Response/Service-Authorization the Type field 808 is set to a code identifying the packet as a Service-Authorization packet.

The Data type field 810 is one octet and specifies the type of data of the Data field 812. According to one embodiment of the EAP-Request/Service-Authorization the type of data may, for example, be Attribute-Value pairs, Must-Show textual string, or XML document. According to one embodiment of the EAP-Response/Service-Authorization the Data type field identifies the type of the signed data, which may, for example, be a PKCS#1 Signature, PKCS#7 signed data, or an XML-Signature. A description of PKCS#1 is found in "PKCS #1: RSA Cryptography Standard", Version 2.0, October 1998, from RSA Laboratories. A description of PKCS#7 is found in "PKCS #7: Cryptographic Message Syntax Standard", Version 1.5, November 1993, from RSA Laboratories. A description of XML-signature is found in the following document by D. Eastlake 3rd, J. Reagle, D. Solo, "(Extensible Markup Language) XML-signature Syntax and Processing", RFC 3275, March 2002.

The Data field 812 may comprise any number of octets. According to one embodiment of the EAP-Request/Service-Authorization the Data field 812 includes said account information, which may, for example, be in the form of Attribute value pairs, a Must-Show textual string, or an XML Document. According to one embodiment of the EAP-Response/Service-Authorization the data field 812 includes said signed account information, which

20

may be signed in accordance with the method specified in the Data type field 810.

The amount of data to be transmitted in a single Service Authorization message may be very large. The
5 service authorization messages sent in a single round may, thus, be larger than the size of a Point-to-Point Protocol Maximum Transmission unit (PPP MTU), a maximum RADIUS packet size of 4096 octets, or even a Multilink Maximum Received Reconstructed Unit (MRRU). As described
10 in IETF RFC 1990, "The PPP Multilink Protocol (MP)", by Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti, August 1996, the multilink MRRU is negotiated via the Multilink MRRU LCP option, which includes an MRRU length field of two octets, and thus can support MRRUs as
15 large as 64 KB.

However, in order to protect against reassembly lockup and denial of service attacks, it may be desirable for an implementation to set a maximum size for one such group of Service Authorization messages. Since a typical
20 certificate chain is rarely longer than a few thousand octets, and no other field is likely to be anywhere near as long, a reasonable choice of maximum acceptable message length might be 64 KB.

If this value is chosen, then fragmentation can be
25 handled via the multilink PPP fragmentation mechanisms described in IETF RFC 1990. While this is desirable, there may be cases in which multilink or the MRRU LCP option cannot be negotiated. As a result, an EAP-Service-Authorization implementation may, according to one
30 embodiment, be arranged to provide its own support for fragmentation and reassembly.

Since EAP is a simple ACK-NAK protocol, fragmentation support can be added in a simple manner. In EAP, fragments that are lost or damaged in transit will
35 be retransmitted, and since sequencing information is provided by the Identifier field in EAP, there is no need for a fragment offset field as is provided in IPv4.

EAP-Service-Authorization fragmentation support may be provided through addition of a flags octet within the EAP-Response and EAP-Request packets, as well as a Service Authorization Message Length field of four octets. For example, flags may include the Length included (L) and More fragments (M) bits. In such case, the L flag may be set to indicate the presence of the four octet Service Authorization Message Length field, and is set for the first fragment of a fragmented Service Authorization message or set of messages. Accordingly, the M flag is set on all but the last fragment. The Service Authorization Message Length field may be four octets, and provides the total length of the Service Authorization message or set of messages that is being fragmented; this may simplify buffer allocation.

When an EAP-Service-Authorization peer receives an EAP-Request packet with the M bit set, it respond with an EAP-Response with EAP-Type=EAP-Service-Authorization and no data. This serves as a fragment Acknowledgement (ACK). The EAP server wait until it receives the EAP-Response before sending another fragment. In order to prevent errors in processing of fragments, the EAP server may increment the Identifier field for each fragment contained within an EAP-Request, and the peer may include this Identifier value in the fragment ACK contained within the EAP-Reponse. Retransmitted fragments may contain the same Identifier value.

Similarly, when the EAP server receives an EAP-Response with the M bit set, it responds with an EAP-Request with EAP-Type=EAP-Service-Authorization and no data. This serves as a fragment ACK. The EAP peer wait until it receives the EAP-Request before sending another fragment. In order to prevent errors in the processing of fragments, the EAP server may use increment the Identifier value for each fragment ACK contained within an EAP-Request, and the peer may include this Identifier

value in the subsequent fragment contained within an EAP-Response.

According to one embodiment an EAP-Service-Authorization implementation that is arranged to provide
5 its own support for fragmentation and reassembly may utilise an EAP-Request/Service-Authorization packet format and an EAP-Response/Service-Authorization packet format described below and showed in Fig. 9.

Regardless of whether the packet is an EAP-
10 Request/Service-Authorization packet or an EAP-Response/Service-Authorization packet the packet comprises a Code field 802, an Identifier field 804, a Length field 806, a Type field 808, a Flags field 902, a Service Authorization Message Length field 904. The Code
15 field 802, the Identifier field 804, the Length field 806, and the Type field 808 may be identical to the corresponding fields described in connection with Fig. 8.

The Flags field 902 may be one octet in length and includes flags for controlling the fragmentation. In one
20 embodiment the Flags field may have the format showed in Fig. 10, in which the characters L, M, and R are one bit and are indicating flags, and:

L = Length included
25 M = More fragments
R = Reserved

The L flag (length included) is set to indicate the presence of the four octet Service Authorization Message
30 Length field, and may be set for the first fragment of a fragmented Service Authorization message or set of messages. The M bit (more fragments) is set on all but the last fragment.

The Service Authorization Message Length field 904
35 may be four octets, and is present only if the L bit is set. This field provides the total length of the Service

23

Authorization or set of messages that is being fragmented.

5 The Service Authorization XXX Message field 906, is a Service Authorization Request Message field in an EAP-Request/Service-Authorization packet and a Service Authorization Response Message field in an EAP-Response/Service-Authorization packet.

10 The Service Authorization Request Message field in an EAP-Request/Service-Authorization packet may include data to be signed, i.e. accounting information, and an indication of the format of said data. This may be implemented in a plurality of ways. For example, the Transport Layer Security (TLS) protocol may be utilized. The TLS protocol and the presentation language of TLS is
15 described in IETF RFC 2246, "The TLS Protocol Version 1.0", by T. Dierks, C. Allen, January 1999. Said format may, for example, indicate a text based string, Attribute-Value pairs, or a XML document.

20 The Service Authorization Response Message field in an EAP-Response/Service-Authorization packet includes the signed data and if necessary an indication of the signing method. The signing methods may, for example, be one of the methods described in connection with Fig. 8.

25

CLAIMS

1. Method in a system for transferring accounting
5 information, said method comprising:
metering data related to a service used by at least
one terminal,
providing the metered data as accounting information
to at least one Extensible Authentication Protocol (EAP)
10 service authorization server,
sending, by means of an Extensible Authentication
Protocol request (EAP-request), a service authorization
request from said at least one EAP service authorization
server to said at least one terminal,
15 digitally signing accounting information, in said at
least one terminal,
including, at said at least one terminal, the
digitally signed accounting information in an Extensible
Authentication Protocol response (EAP-response), and
20 sending the digitally signed accounting information
to an AAA-server.
2. Method according to claim 1, wherein the act of
providing the metered data to the at least one EAP
service authorization server is performed by means of
25 internal communication within a device comprising both
said at least one metering server and said at least one
EAP service authorization server.
3. Method according to claim 1, wherein the act of
providing the metered data to the at least one EAP
30 service authorization server is performed by means of
network communication between a device comprising said at
least one metering server and a device comprising said at
least one EAP service authorization server.
4. Method according to any one of claims 1-3,
35 wherein the at least one metering server is included in
an access point, and wherein said EAP-request for service
authorization and said EAP-response including signed

25

accounting information is received and sent by the terminal via said access point.

5. Method according to claim 4, wherein said receiving and sending by said at least one terminal from/to said access point is performed by means of Wireless Lokal Area Network (WLAN) communication.

6. Method according to any one of claims 1-5, wherein said sending of a service authorization request comprises including the accounting information, provided to said at least one EAP service authorization server, in said EAP-request for service authorization, and wherein said method further comprises verifying, performed by said at least one terminal, the accounting information received from said at least one EAP service authorization server before the step of digitally signing accounting information is performed, wherein the accounting information that is signed is the verified accounting information.

7. Method according to any one of claims 1-5, wherein said sending of a service authorization request comprises including the accounting information, provided to said at least one EAP service authorization server, in said EAP-request for service authorization, and wherein said method further comprises verifying, performed by the user of said at least one terminal, the accounting information received from said at least one EAP service authorization server before the step of digitally signing accounting information is performed, wherein the accounting information that is signed is the verified accounting information.

8. Method according to any one of claims 1-5, wherein said sending of a service authorization request does not comprise any step of including the accounting information provided to said at least one EAP service authorization server in said EAP-request, and wherein said digitally signing of accounting information

26

comprises digitally signing accounting information collected by said at least one terminal.

9. Method according to any one of claims 1-8, wherein said step of sending the verified and digitally signed accounting information to the AAA-server comprises:

10 sending the digitally signed accounting information from said at least one terminal to said at least one EAP service authorization server by means of said EAP-response,

verifying the signature of the digitally signed accounting information at the at least one EAP service authorization server, and

15 sending the digitally signed accounting information from said at least one EAP service authorization server to the AAA server.

10. Method according to any one of claims 1-9, wherein the digitally signing is performed by means of a public key algorithm.

20 11. System for transferring accounting information, said system comprising:

a metering server for metering data related to a service,

25 an Extensible Authentication Protocol (EAP) service authorization server including a generator for generating Extensible Authentication Protocol requests (EAP-request) for service authorizations, and a network connection means,

30 a terminal including a signer arranged to digitally sign verified accounting information, an Extensible Authentication Protocol response (EAP-response) generator arranged to insert digitally signed accounting information in EAP-responses, and a network connection means, and

35 an Authentication Authorization Accounting (AAA) server arranged to manage accounting information relating to at least one terminal.

12. System according to claim 11, wherein the metering server and the EAP service authorization server are arranged in the same device.

13. System according to claim 11, wherein the
5 metering server and the EAP service authorization server are arranged in different devices.

14. System according to any one of claims 11-13, further comprising an access point, wherein the access point includes said metering server.

15. System according to claim 14, wherein said at
10 least one terminal is a Wireless Local Area Network (WLAN) enabled terminal and said at least one access point is a WLAN access point.

16. System according to any one of claims 11-15,
15 wherein said generator for generating Extensible Authentication Protocol request (EAP-request) service authorizations is arranged to insert accounting information of at least one terminal in EAP-requests for service authorizations.

17. System according to any one of claims 11-16,
20 wherein said terminal further comprises a verifier arranged to verify accounting information received from a service authorization server.

18. System according to any one of claims 11-17,
25 wherein said EAP service authorization server further comprises a signature verifier for verifying signatures of terminals, and an accounting message generator for generating accounting messages to be sent to said AAA-server.

19. Method in a terminal, said method comprising:
30 collecting data corresponding to accounting information relevant for at least one service presently utilized in the terminal,

receiving an Extensible Authentication Protocol
35 request (EAP-request) for service authorization, digitally signing accounting information, and

28

sending the digitally signed accounting information in an Extensible Authentication Protocol response (EAP-response).

20. Method according to claim 19, wherein the
5 accounting information that is digitally signed in the step of digitally signing accounting information is the data collected in the step of collecting data corresponding to accounting information.

21. Method according to claim 19, wherein said EAP-
10 request for service authorization, received in the step of receiving an EAP-request for service authorization, includes accounting information relevant for said at least one service presently utilized in the terminal.

22. Method according to claim 21, the method further
15 comprising:

comparing said received accounting information with the collected data, and

if the collected data corresponds with the accounting information then performing said steps of
20 digitally signing accounting information and sending the digitally signed accounting information.

23. Method according to any one of claims 19-22, wherein receiving an EAP-request and sending an EAP-response is performed over a Wireless Local Area Network
25 connection.

24. Method according to any one of claims 19-23, wherein the act of digitally signing comprises encrypting said verified accounting information by means of a public key cryptosystem.

30 25. Terminal comprising:

a collector arranged to collect data corresponding to accounting information relevant for at least one service presently utilized in the terminal,

a signer arranged to digitally sign accounting
35 information,

29

an Extensible Authentication Protocol response (EAP-response) generator arranged to insert digitally signed accounting information in EAP-responses, and
a network connection means.

5 26. Terminal according to claim 25, further comprising a comparing device arranged to compare the collected data with received accounting information.

27. Terminal according to any one of claim 25 or claim 26, wherein said network connection means is a
10 Wireless Local Area Network (WLAN) connection means for connecting said terminal to a WLAN.

28. Terminal according to any one of claim 25 or claim 27, further comprising a public key cryptosystem encryption algorithm for signing verified accounting
15 information.

29. Method in an Extensible Authentication Protocol (EAP) service authorization server, said method comprising:

receiving accounting information related to at least
20 one terminal,

sending, to at least one terminal, an Extensible Authentication Protocol request (EAP-request) for ordering service authorization,

receiving an Extensible Authentication Protocol
25 response (EAP-response) including signed accounting information, which has been signed in the at least one terminal,

providing an Authentication Authorization Accounting server with the signed accounting information.

30 30. Method according to claim 29, wherein said accounting information is received via a network.

31. Method according to claim 29, wherein said accounting information is received via internal communication means of a device in which said EAP service
35 authorization server is included.

32. Method according to any one of claims 29-31, further comprising:

inserting said received accounting information in the EAP-request, before the steps of sending an EAP-request and receiving an EAP-response is performed, for ordering service authorization.

5 33. Method according to any one of claims 29-32, wherein the signature of said signed accounting information is verified by means of a public key cryptosystem algorithm.

10 34. Method according to any one of claims 29-33, further comprising verifying the signed accounting information before the signed accounting information is provided to said AAA server.

15 35. Method according to any one of claims 29-34, wherein said EAP-response is received from a terminal via a Wireless Local Area Network (WLAN).

36. Extensible Authentication Protocol (EAP) service authorization server comprising:

an accounting information receiver for receiving accounting information relating to at least one terminal,

20 an Extensible Authentication Protocol request (EAP-request) generator arranged to generate EAP-requests for service authorizations,

an extractor for extracting digitally signed accounting information from an Extensible Authentication Protocol response (EAP-response) received,

25 an accounting message generator for generating a message, complying with an Authentication Authorization Accounting (AAA) protocol, including said digitally signed accounting information, and

30 a network connection means.

37. EAP service authorization server according to claim 36, wherein said EAP service authorization server is comprised in an access point.

35 38. EAP service authorization server according to any one of claim 36 or 37, wherein the EAP-request generator further is arranged to insert accounting

31

information relating to services used by at least one terminal in an EAP-request.

39. EAP service authorization server according to any one of claims 36-38, further comprising at least one
5 public key for decryption of a signed message.

40. Computer program directly loadable into the internal memory of a terminal, the computer program comprising software code portions for performing the method of any one of claims 19-24.

10 41. Computer program directly loadable into the internal memory of an Extensible Authentication Protocol (EAP) service authorization server, the computer program comprising software code portions for performing the method of any one of claims 29-35.

15 42. Extensible Authentication Protocol response (EAP-response) packet comprising digitally signed accounting information relating to a terminal.

43. EAP-response packet in accordance with claim 42, wherein the packet includes a Data type field specifying
20 the signing method used for signing the accounting information, and a Data field including the signed accounting information, which is signed by means of the method specified in the Data type field.

ABSTRACT

A method in a system for transferring accounting
5 information, a system for transferring accounting
information, a method in a terminal, a terminal, a method
in an Extensible Authentication Protocol (EAP) service
authorization server, an EAP service authorization
server, a computer program, a computer program, an
10 Extensible Authentication Protocol response (EAP-
response) packet.

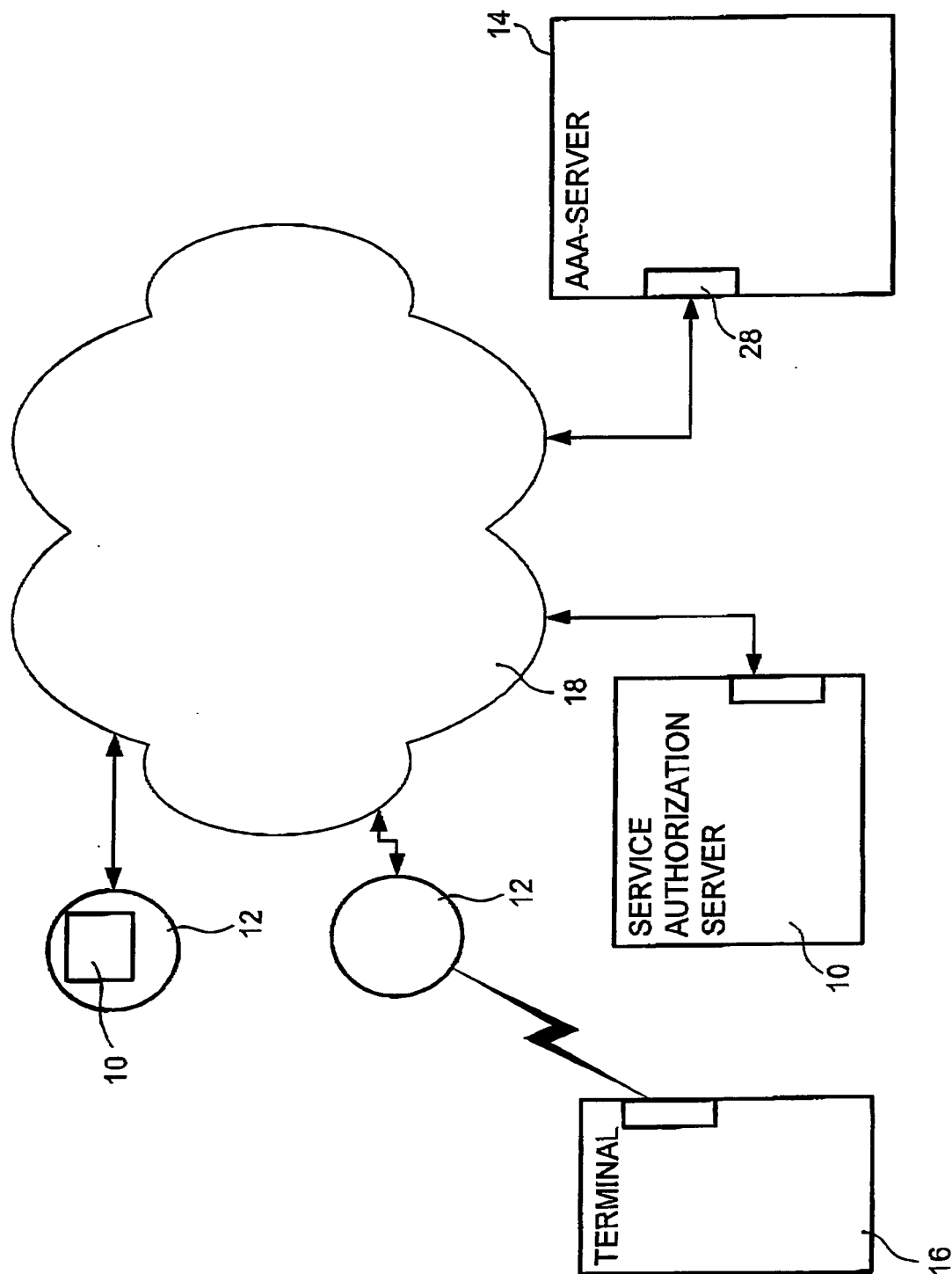
The method in a system comprises:

metering data related to a service used by at least
one terminal,
15 providing the metered data as accounting information
to at least one Extensible Authentication Protocol (EAP)
service authorization server,
sending, by means of an Extensible Authentication
Protocol request (EAP-request), a service authorization
20 request from said at least one EAP service authorization
server to said at least one terminal,
digitally signing accounting information, in said at
least one terminal,
including, at said at least one terminal, the
25 digitally signed accounting information in an Extensible
Authentication Protocol response (EAP-response), and
sending the digitally signed accounting information to an
AAA-server.

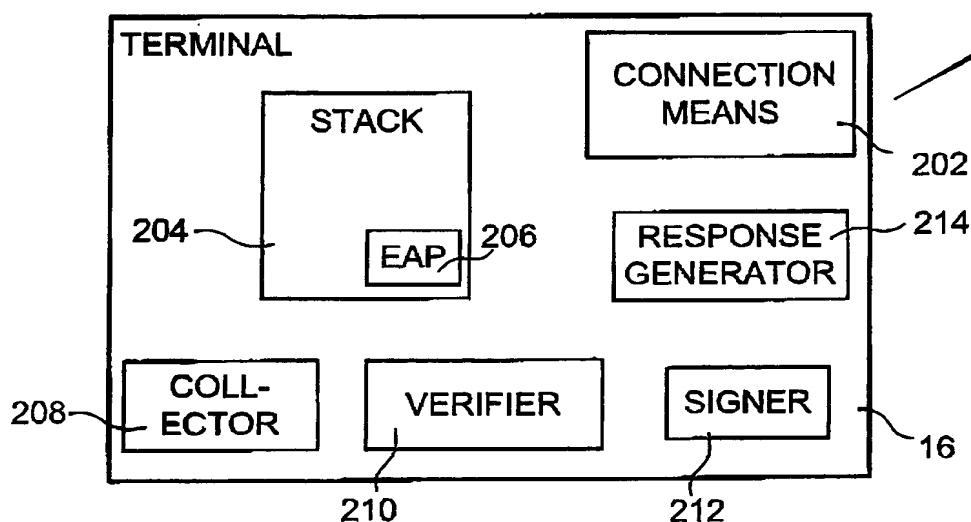
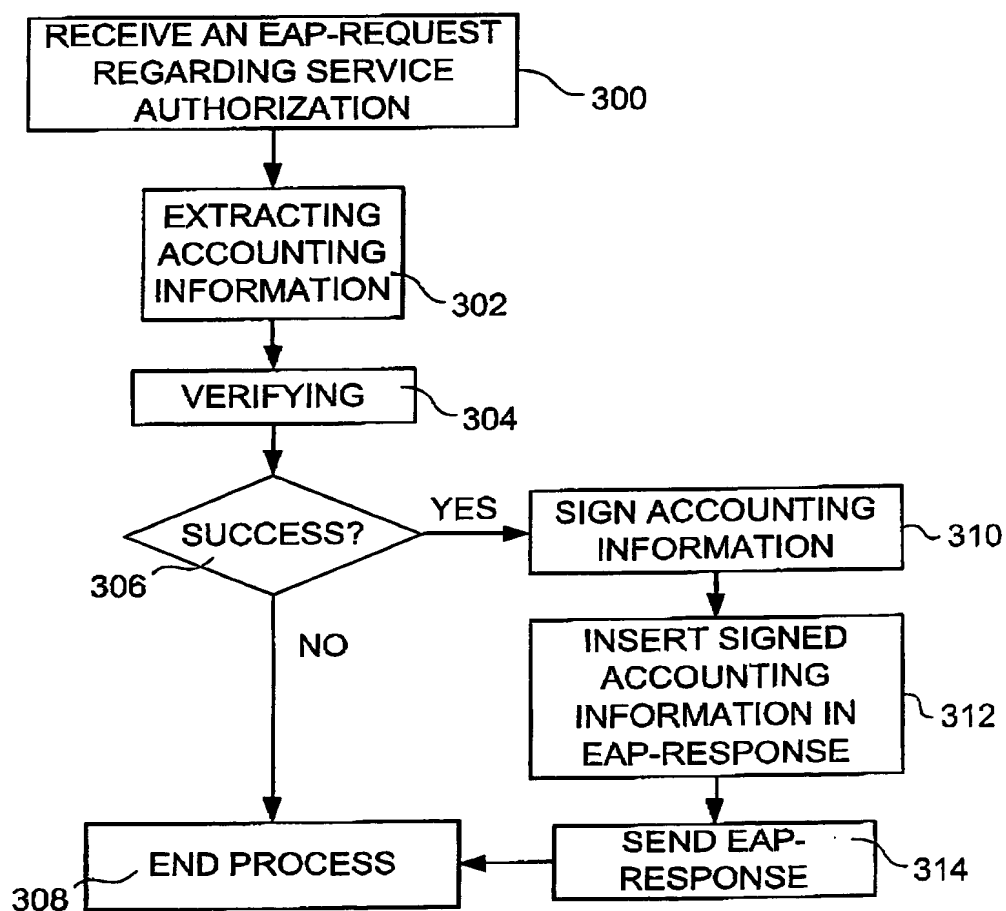
30 [Elected for publication: Fig. 6]^A

130

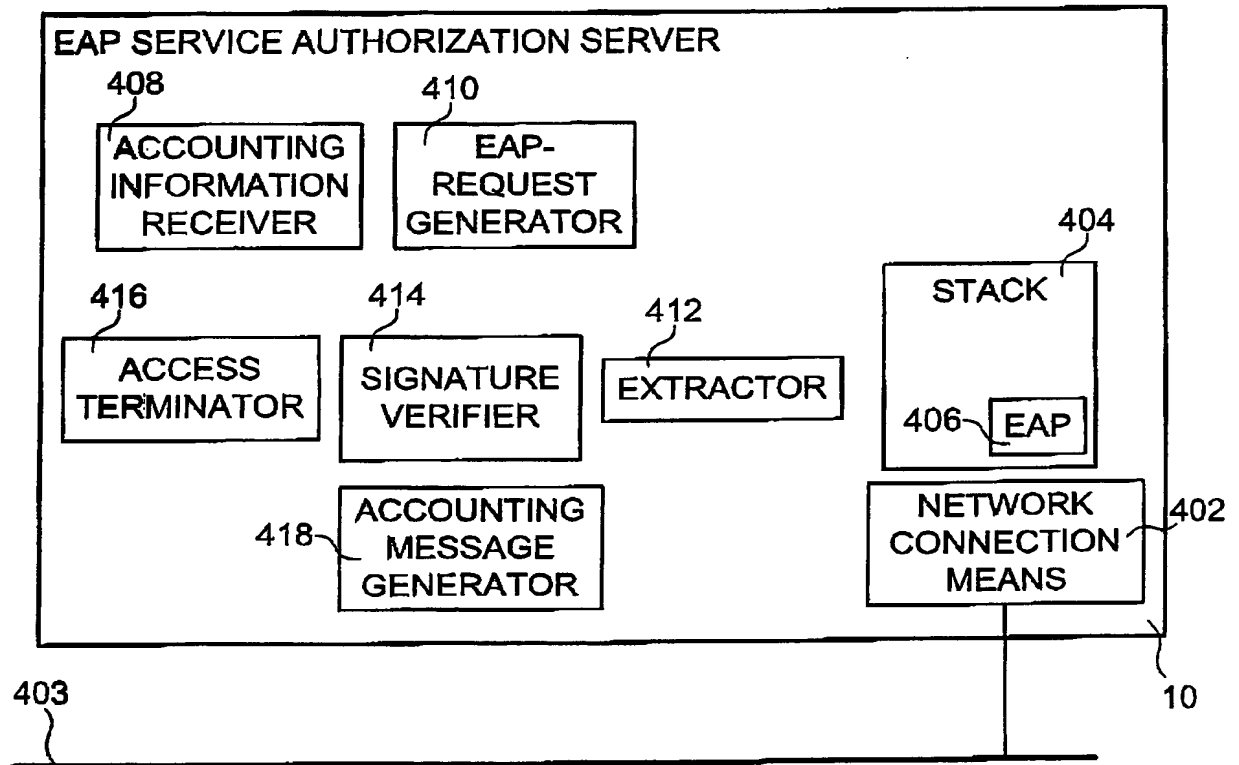
1/7



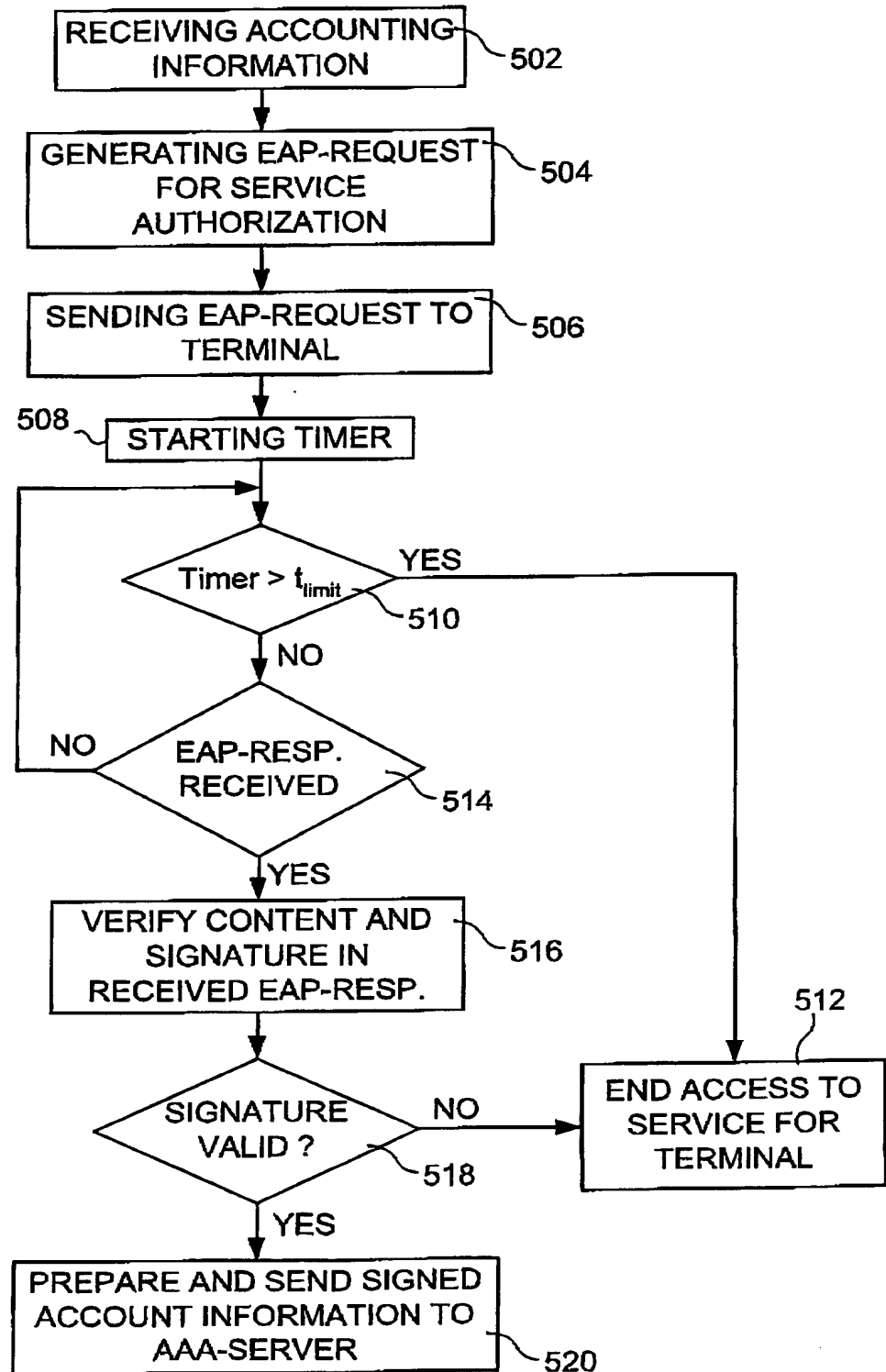
2/7

**FIG 2****FIG 3**

3/7

**FIG 4**

4/7

**FIG 5**

5/7

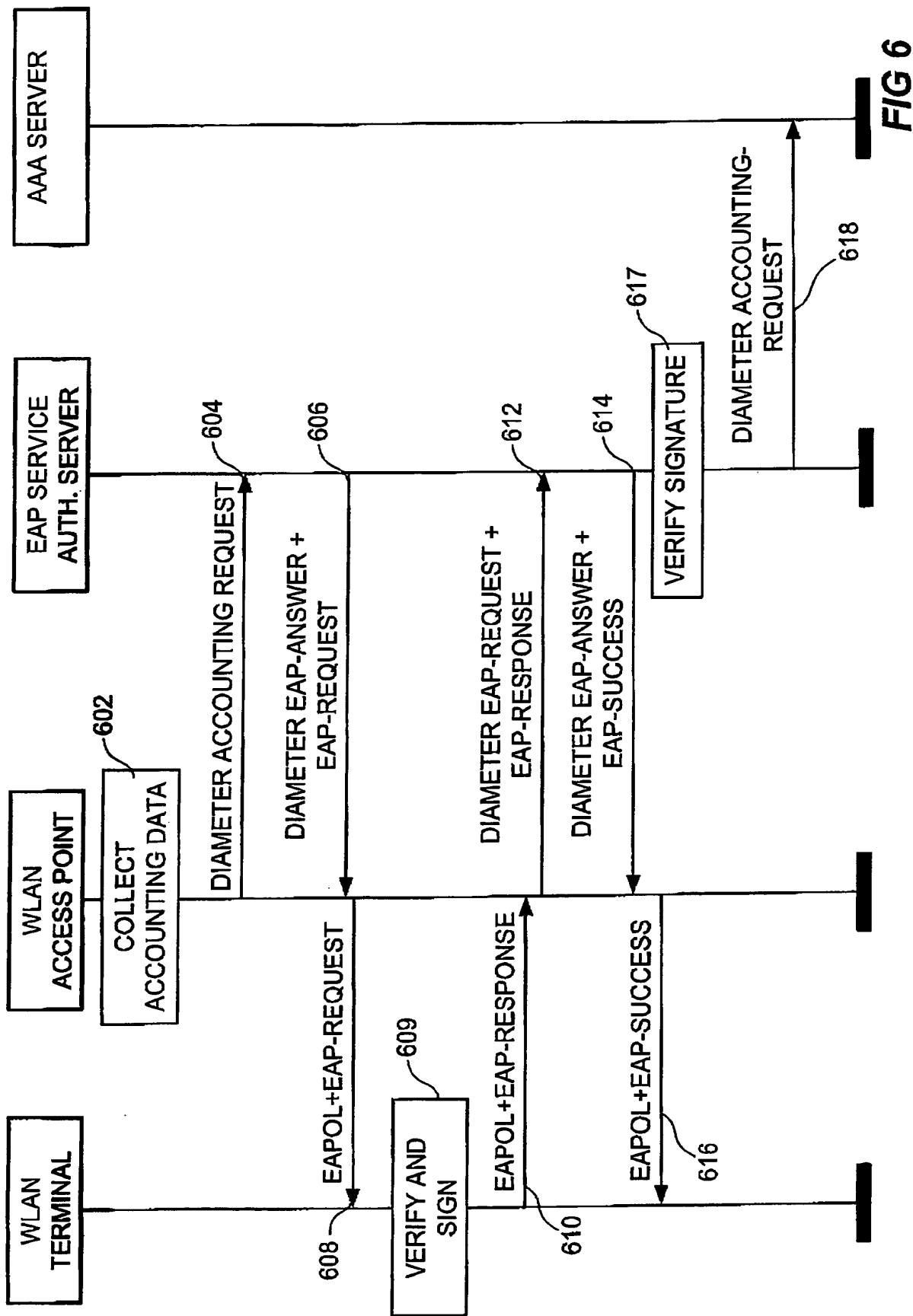


FIG 6

6/7

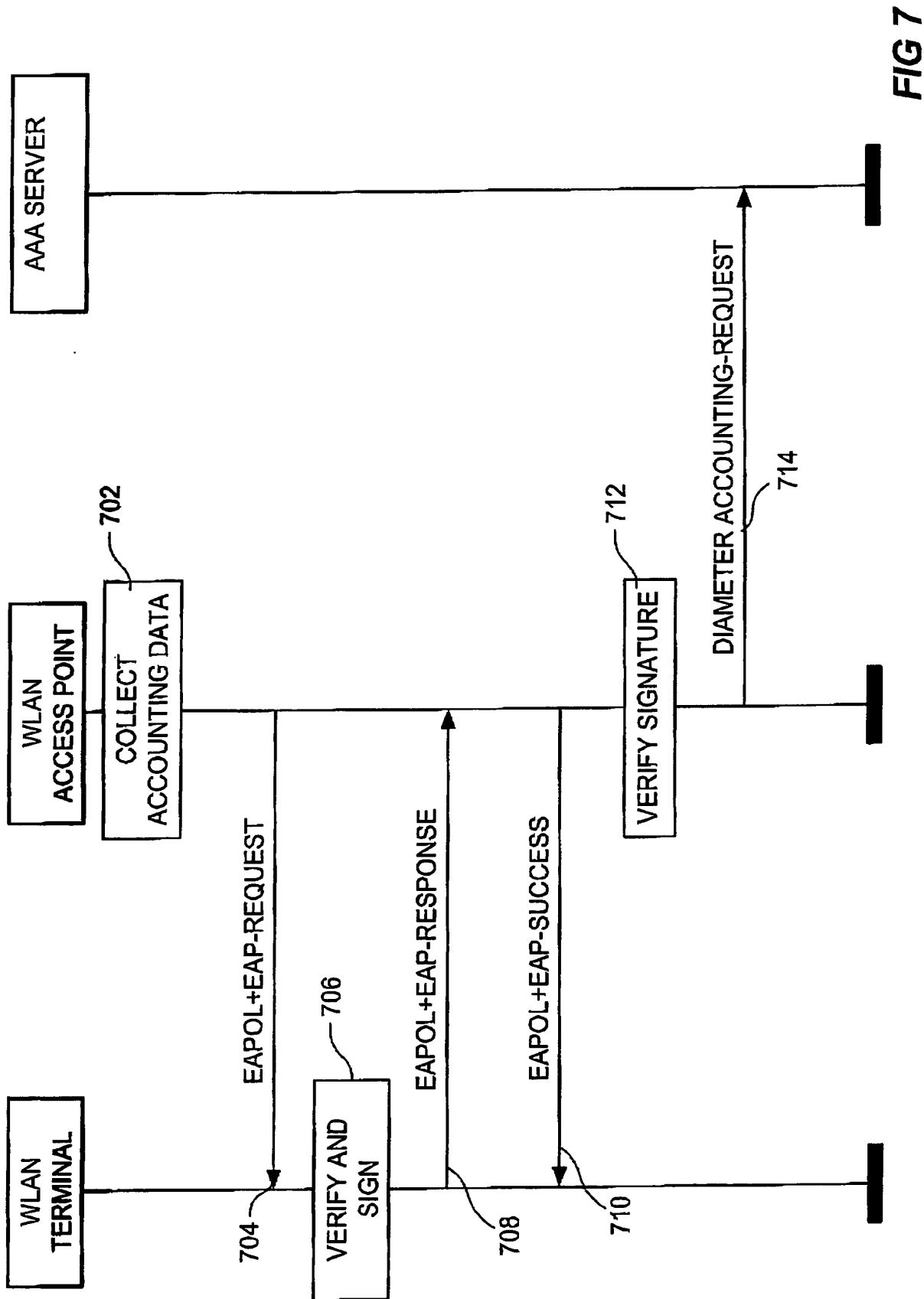


FIG 7

